REMARKS

Applicants thank the Examiner for the careful and thorough examination of the present application. The Examiner is also thanked for properly withdrawing the prior rejections. The Examiner is further thanked for the telephonic interview of July 8, 2009, during which the current claim rejections were discussed. Independent Claim 21 has been amended to correct a minor typographical error. Independent Claims 1, 12, 21, 26, and 36 have been amended to further define over the prior art and along the lines discussed during the telephonic interview. The patentability of the claims is discussed below.

I. The Claimed Invention

Amended independent Claim 1 is directed to a cryptographic device including a cryptographic module and a communications module coupled thereto. The cryptographic module includes a user network interface, a host network processor coupled to the user network interface, and a cryptographic processor coupled to the host network processor. The communications module includes a network communications interface coupled to the cryptographic processor. The host network processor generates cryptographic processor command packets for the cryptographic processor, each including an address portion for addressing the cryptographic processor and a data portion. Each data portion includes one of unencrypted

data and command packets for the communications module. The host network processor also encapsulates the command packets for the communications module in the data portions of the cryptographic processor command packets.

The cryptographic processor determines if a given cryptographic processor command packet includes the encapsulated command packet and based thereon strips the address portion from the cryptographic processor command packet and passes the encapsulated communications module command packet to the communications module without performing cryptographic processing thereon. The cryptographic processor also determines if another given cryptographic processor command packet includes the unencrypted data packet and encrypts the unencrypted data packet and passes the encrypted data packet to the communications module.

Amended independent Claim 21 is a method counterpart to amended independent Claim 1. Amended independent Claim 26 is a system counterpart to amended independent Claim 1 further reciting the host network processor formatting the data portions based upon the simple network management protocol. Amended independent Claim 36 is directed to a related cryptographic processor. Independent Claims 21, 26, and 36 have been amended similar to amended independent Claim 1.

Amended independent Claim 12 is directed to a cryptographic device, as recited in amended independent Claim 1, further reciting the user network interface as a Local Area

Network (LAN) interface, the command packets as Ethernet command packets, and the host network processor formatting the data portions based upon the simple network management protocol. Independent Claim 12 has been amended similar to amended independent Claim 1.

II. The Claims Are Patentable

The Examiner rejected independent Claims 1, 12, 21, 26 and 36, based on a combination of Dellmo et al., and Forslow. Independent Claim 12 was rejected further in view of Stevens. Dellmo et al. is directed to a secure wireless LAN device including a housing, a wireless transceiver carried by the housing, and a cryptography circuit carried by the housing. A media access controller (MAC) is included and implements a predetermined wireless LAN MAC protocol. The cryptography circuit includes a cryptography processor, and a control gateway circuit connected to the MAC and the wireless transceiver. The secure wireless LAN device also includes a user network interface carried by the housing and connected to the MAC.

The Examiner correctly recognized that Dellmo et al. fails to disclose the host network processor generating cryptographic processor command packets for the cryptographic processor each including an address portion for addressing the cryptographic processor circuit and a data portion, and encapsulating command packets for the communications module in

the data portions of the cryptographic processor command packets. The Examiner further correctly recognized that Dellmo et al. fails to disclose the cryptographic processor stripping the address portion from each cryptographic processor command packet and passing the encapsulated communications module command packets to the communications module without performing cryptographic processing thereon. The Examiner turned to Forslow to support these critical deficiencies.

Forslow is directed to a public mobile data communications network. More particularly, Forslow discloses mobile node data access to the Internet and data access to the mobile node from the Internet even when a point of attachment of the mobile node to the public mobile access data network changes.

Independent Claims 1, 12, 21, 26, and 36 have been amended to recite each data portion of the cryptographic processor command packet includes one of unencrypted data and command packets for the communications module. Independent Claims 1, 12, 21, 26, and 36 have also been amended to recite the cryptographic processor determining if a given cryptographic processor command packet includes the encapsulated command packet and based thereon stripping the address portion from the cryptographic processor command packet and passing the encapsulated communications module command packet to the communications module without performing cryptographic processing thereon. Independent Claims 1, 12, 21, 26, and 36

have further been amended to recite the cryptographic processor also determines if another given cryptographic processor command packet includes the unencrypted data packet and encrypting the unencrypted data packet and passing the encrypted data packet to the communications module.

Applicants submit that even a selective combination of the prior art fails to produce the claimed invention. More particularly, a selective combination of Dellmo et al. and Forslow fails to disclose the cryptographic processor determining if a given cryptographic processor command packet includes the encapsulated command packet and based thereon stripping the address portion from the cryptographic processor command packet and passing the encapsulated communications module command packet to the communications module without performing cryptographic processing thereon.

The Examiner contended that the cryptography circuit 70 of Dellmo et al. corresponds to the claimed cryptographic processor. Applicants submit that Dellmo et al. fails to disclose the cryptography circuit 70 determining if a given cryptographic processor command packet includes an unencrypted data packet or a cryptographic processor command packet. Instead, Dellmo et al. discloses the cryptography circuit 70 encrypting both address and data information for transmission. (See Dellmo et al., paragraph 0039).

Forslow similarly fails to supply this critical deficiency. Forslow is not directed to cryptography and makes

no mention of cryptography. Moreover, Forslow makes mention of only one type of packet. That is, Forslow discloses the data packet 32 being encapsulated in the encapsulated packet 38. "The IP packet 32 is now the payload portion of the encapsulated packet 38 which is routed to the foreign agent using the care-of address for the mobile node." (See Forslow, Col. 9, lines 16-19, and Fig. 2). Thus, the foreign agent 20, which the Examiner contended also corresponds to the claimed cryptographic processor, simply does not determine whether a given cryptographic processor command packet includes an unencrypted data packet or a cryptographic processor command packet, and does not perform encryption. Accordingly, amended independent Claims 1, 21, 26, and 36 are patentable for at least this reason alone.

Still further, Applicants submit that even a selective combination of the prior art fails to disclose the cryptographic processor also determining if another given cryptographic processor command packet includes the unencrypted data packet and encrypting the unencrypted data packet and passing the encrypted data packet to the communications module. As described in detail above, Dellmo et al. merely teaches the cryptography circuit 70 encrypting both address and data information for transmission. (See Dellmo et al., paragraph 0039). Nowhere does Dellmo et al. teach or suggest the cryptographic processor also determining if another given cryptographic processor command packet includes the unencrypted

data packet and encrypting the unencrypted data packet and passing the encrypted data packet to the communications module. For the reasons described in greater detail above, Forslow also fails to supply these critical deficiencies, as Forslow is not directed to cryptography and makes no mention of cryptography. Accordingly, amended independent Claims 1, 21, 26, and 36 are patentable also for this reason.

Applicants further submit that the Examiner's combination of references is improper as a person having ordinary skill in the art would not turn to the public mobile data communications network that provides mobility management for mobile nodes in an attempt to combine with a secure wireless LAN device. More particularly, a person skilled in the art would not combine a communications network that makes no mention of encryption nor performs any encryption, as in Forslow, to combine with a secure device, as in Dellmo et al. Indeed, such a combination may compromise the security of the secure device. Accordingly, amended independent Claims 1, 21, 26, and 36 are patentable for this reason also.

The Examiner rejected independent Claim 12 in further view of Stevens et al. Stevens et al., which is cited as disclosing an SNMP protocol adds nothing to the critical deficiencies of Dellmo et al. and Forslow, as described in detail above.

Accordingly, it is submitted that amended independent Claims 1, 12, 21, 26, and 36 are patentable over the prior art.

Their respective dependent claims, which recite yet further distinguishing features, are also patentable over the prior art and require no further discussion herein.

III. Conclusion

In view of the amendments and arguments presented above, it is submitted that all of the claims are patentable. Accordingly, a Notice of Allowance is respectfully requested in due course. If the Examiner determines any remaining informalities exist, he is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,

DAVID S. CARUS
Reg. No. 59,291
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330
407-841-2343 fax
Attorney for Applicants